

Technical Safety Concept Lane Assistance

**Document Version: 1.1**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 12.01.2019 | 1.0 | Michael Ikemann | Initial technical safety conception |
| 13.0.1.2019 | 1.1 | Michael Ikemann | Refinement |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

[Document history](#_1t3h5sf)

[Table of Contents](#_ktt3lgighckp)

[Purpose of the Technical Safety Concept](#_fulgh8sf1ocg)

[Inputs to the Technical Safety Concept](#_757cx6xm46zb)

[Functional Safety Requirements](#_2f9rjqxbsp2)

[Refined System Architecture from Functional Safety Concept](#_qp3s9pvua9mt)

[Functional overview of architecture elements](#_cqb49updinx4)

[Technical Safety Concept](#_mx8us8onanqo)

[Technical Safety Requirements](#_lnxjuovv6kca)

[Refinement of the System Architecture](#_74udkdvf7nod)

[Allocation of Technical Safety Requirements to Architecture Elements](#_g2lqf7kmbspk)

[Warning and Degradation Concept](#_4w6r8buy4lrp)

# Purpose of the Technical Safety Concept

The technical safety concept describes in detail and from a low level, technical perspective how the requirements can be satisfied on the technical sight and which architectural requirements need to be fulfilled to do so.

# Inputs to the Technical Safety Concept

## Functional Safety Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  01-01 | Bad weather conditions and incorrectly working sensors are detected and the user will be informed. | B | 0.1s | The system will be disabled and the user informed via dashboard. |
| Functional  Safety  Requirement  01-02 | The detection data is provided in intervals of 10 Hz. In case of lost messages the system will automatically be disabled. | B | 0.1s | The system will be disabled and the user informed via dashboard. |
| Functional  Safety  Requirement  02-01 | If the current situation can be detected reliably anymore the system should slow down the car and instantly inform the driver. | B | 0.1s | The system will temporarily disabled until the situation normalized. |

## Refined System Architecture from Functional Safety Concept

### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Is located behind the wind shield, captures images and sends them as stream to the CS ECU. |
| Camera Sensor ECU - Lane Sensing | Detects lanes by analysing the camera image and applying edge detection filters. Forwards the information of the detect lanes and the confidence to the torque request generator. |
| Camera Sensor ECU - Torque request generator | If the LKA is enabled and the lanes could confidentially be identified it will create torque requests so the vehicle will stay in the lane’s center.  If the situation is unsafe it will disable the LKA temporarily and inform the user about this state by sending the status to the CD ECU. |
| Car Display | Visualizes the vehicle’s current state. |
| Car Display ECU - Lane Assistance On/Off Status | Visualizes if the lane assistance is currently enabled using a symbolic light. |
| Car Display ECU - Lane Assistant Active/Inactive | Visualizes if the lane assistance is currently active using a symbolic light. |
| Car Display ECU - Lane Assistance malfunction warning | Notifies the user if there is any malfunction, for example because of internal system errors or a blocked sensor, for example caused due to weather conditions. |
| Driver Steering Torque Sensor | Detects the driver’s steering torque. The torque is then sent to the EPS and amplified there. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Calculated the factor by which the driver’s torque shall be scaled such as current speed and forwards it to the final torque system. |
| EPS ECU - Normal Lane Assistance Functionality | Receives the computed values from the Torque Request Generator and forwards it to the Lane Keeping Assistant Safety Functionality for verification. |
| EPS ECU - Lane Departure Warning Safety Functionality | Verifies that the torque requested by the NLF is within given bounds of up to MAX\_TORQUE and limits it if required. Zeroes the torque in case of detected functional errors. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Verifies that the torque requested by the NLF is within given bounds of up to MAX\_TORQUE and limits it if required. Zeroes the torque in case of detected functional errors. |
| EPS ECU - Final Torque | Receives the final torque and forwards it to the steering motor. |
| Motor | Applies the torque to the steering mechanically to turn the car’s wheel left or right. |

# Technical Safety Concept

## Technical Safety Requirements

**Lane Departure Warning (LDW) Requirements:**

Functional Safety Requirement 01-01 with its associated system elements

(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-01 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | The LDW safety component shall ensure that the amplitude of the 'LDW\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Torque\_Amplitude. | C | 50ms | LDW\_SAFETY Software | The LDW torque amplitude request shall be set to zero |
| Technical  Safety  Requirement  02 | As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light. | C | 50ms | LDW\_SAFETY Software | The LDW torque amplitude request shall be set to zero |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW\_Torque\_Request' shall be set to zero. | C | 50ms | LDW\_SAFETY Software | The LDW torque amplitude request shall be set to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | C | 50ms | Data Transmission Integrity Check | The LDW torque amplitude request shall be set to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Safety Startup | The LDW torque amplitude request shall be set to zero |

Functional Safety Requirement 01-2 with its associated system elements

(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | The LDW safety component shall ensure that the frequency of the 'LDW\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Torque\_Amplitude | C | 50ms | LDW\_SAFETY Software | | The LDW torque amplitude request shall be set to zero |
| Technical  Safety  Requirement  02 | As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light. | C | 50ms | LDW\_SAFETY Software | | The LDW torque amplitude request shall be set to zero |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW\_Torque\_Request' shall be set to zero. | C | 50ms | LDW\_SAFETY Software | | The LDW torque amplitude request shall be set to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | C | 50ms | Data Transmission Integrity Check | | The LDW torque amplitude request shall be set to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Safety Startup | | The LDW torque amplitude request shall be set to zero |

**Lane Keeping Assistance (LKA) Requirements:**

Functional Safety Requirement 02-1 with its associated system elements

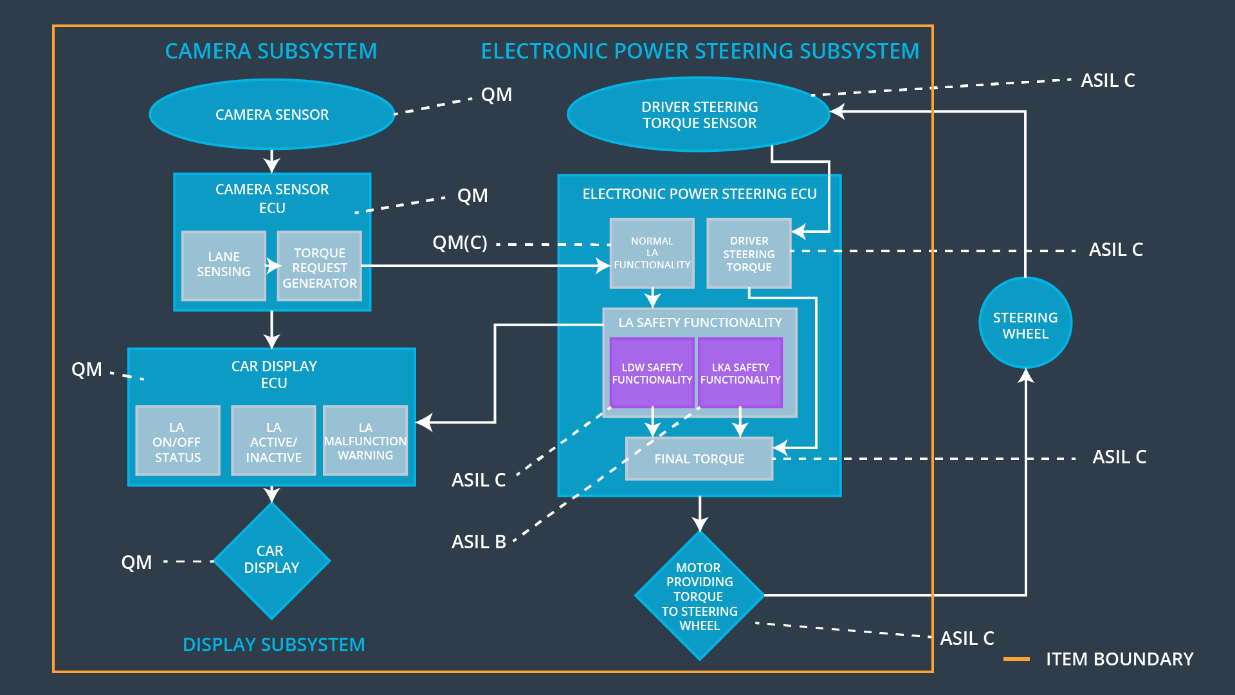
(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  01 | The LKA needs to ensure that the LKA\_Torque signal is only send to the FINAL TORQUE unit above a given threshold for a limited amount of time | C | 500ms | LKA\_SAFETY Software | The LDW torque amplitude request shall be set to zero |
| Technical  Safety  Requirement  02 | As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light. | C | 500ms | LKA\_SAFETY Software | The LDW torque amplitude request shall be set to zero |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA\_Torque\_Request' shall be set to zero. | C | 500ms | LKA\_SAFETY Software | The LDW torque amplitude request shall be set to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LKA\_Torque\_Request' signal shall be ensured. | C | 500ms | Data Transmission Integrity Check | The LDW torque amplitude request shall be set to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Safety Startup | The LDW torque amplitude request shall be set to zero |

## Refinement of the System Architecture



## Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated in the Electronic Power Steering Unit.

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Disabled until next motor start. | CRC checksum errors in communication and or no data provided at 10 Hz rate as required. | LDW disabled. | Error light in dashboard. |
| WDC-02 | Disabled temporarily till situation is safe again. | Too many, none or contradictionary lanes detected. | LKA temporarily disabled. | Inactivity visualized in dashboard. |